Samsung NVMe TCG Opal SSC SEDs PM1743 Series

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

H/W Version: MZCLO1T9HCJR-00AMZ, MZCLO3T8HBLT-00AMZ,
MZCLO7T6HBLA-00AMZ

F/W Version: OPP9TA6A

Revision History

Version	Change
1.0	Initial Version
1.1	Addressing CMVP comments.

Table of Contents

I. Introduction

I.1. Scope

This document is a non-proprietary Security Policy for the **Samsung NVMe TCG Opal SSC SEDs PM1743 Series**, hereinafter referred to as the “cryptographic module” or “module.” The SSD (Solid State Drive) satisfies all applicable FIPS 140-3 security level 1 requirements for a ‘Hardware Module,’ supporting TCG Opal SSC-based SED (Self-Encrypting Drive) features designed to protect against unauthorized access to user data stored in its NAND Flash memories. The built-in AES hardware engines in the cryptographic module’s controller provide on-the-fly encryption and decryption of user data without performance loss. The SED’s design also enables instantaneous sanitization of user data via cryptographic erase.

I.2. Acronyms

Acronym	Description
CPU	Central Processing Unit (ARM-based)
CTRL	Controller
DRAM I/F	Dynamic Random Access Memory Interface
LBA	Logical Block Address
MEK	Media Encryption Key
MSID	Manufactured SID (Security Identifier)
NAND I/F	NAND Flash Interface
PMIC	Power Management Integrated Circuit
ROM	Read Only Memory
NVMe	Non-Volatile Memory Host Controller Interface Specification
SED	Self-Encrypting Drive
SSC	Security Subsystem Class
SSP	Sensitive Security Parameter
TCG	Trusted Computing Group

Table 1. Acronyms

1. General

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A

Table 2. Security Levels

2. Cryptographic Module Specification

2.1. Cryptographic Boundary

This firmware version, within the scope of this validation, must be validated through the FIPS 140-3 CMVP. Any other firmware loaded into this module is beyond the scope of this validation and requires a separate FIPS 140-3 validation.

The following photographs depict the top and bottom views of the cryptographic module. The multiple-chip standalone cryptographic module comprises of both hardware and firmware components, all enclosed within two aluminum alloy cases. These cases serve as the cryptographic boundary of the module.

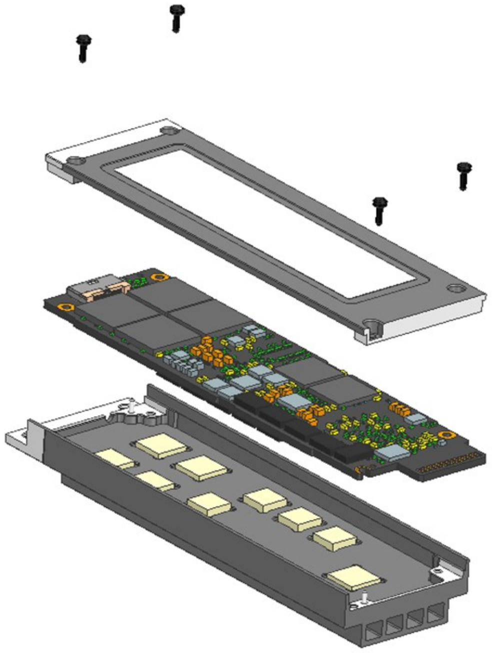

Figure 1. Specification of the Samsung SSD NVMe TCG Opal SSC SEDs PM1743 Series Cryptographic Boundary

The PM1743 series utilizes a single-chip controller with an NVMe interface on the system side and internally integrates Samsung NAND flash. The following figure illustrates the operational environment of the module.

The cryptographic boundary, shown in Figure 2 below, is represented by the black box that encloses the components of the module.

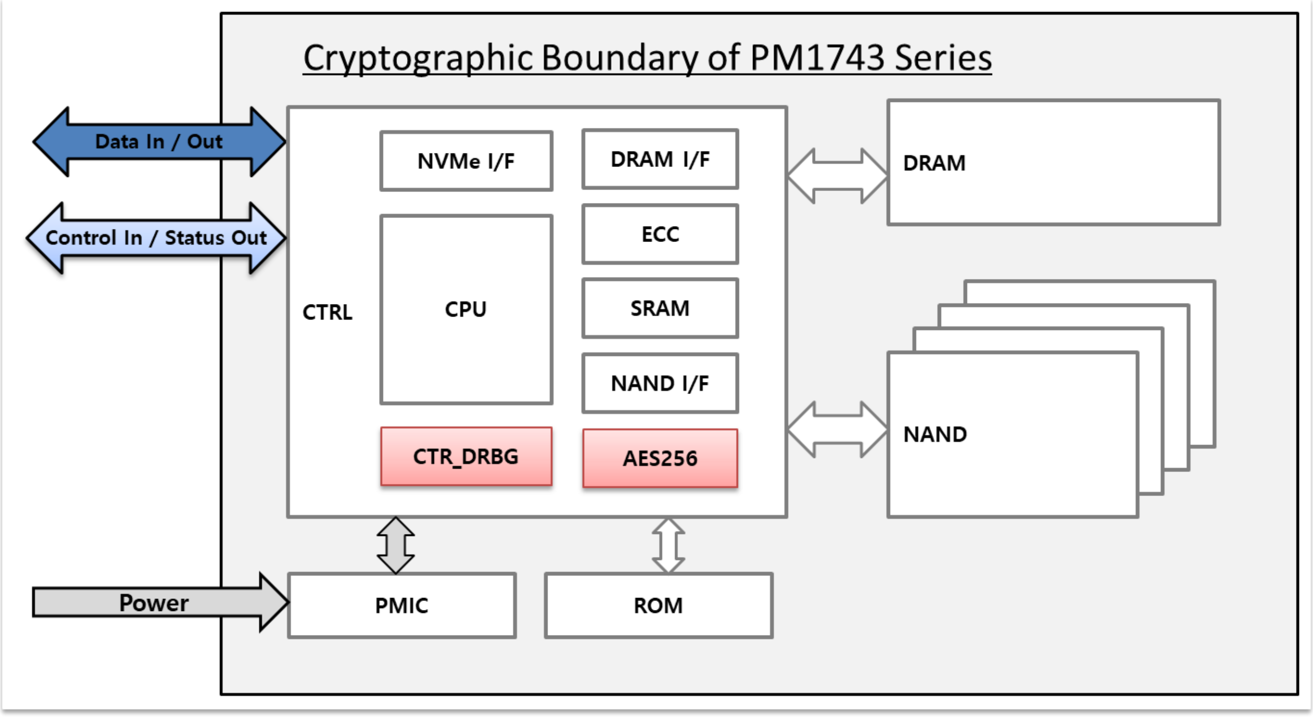

Figure 2. Block Diagram for Samsung SSD NVMe TCG Opal SSC SEDs PM1743 Series

2.2. Version information

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
PM1743	MZCLO1T9HCJR-00AMZ	OPP9TA6A	1.92TB
	MZCLO3T8HBLT-00AMZ		3.84TB
	MZCLO7T6HBLA-00AMZ		7.68TB

Table 3. Cryptographic Module Tested Configuration

2.3. Cryptographic Functionality

2.3.1. Approved Algorithm[1]

The cryptographic module supports the following Approved algorithms for secure data storage:

CAVP Cert	Algorithm and Standard	Mode/ Method	Description/ Key Size(s)/ Key Strength(s)	Use/Function
A2247	AES-ECB / FIPS 197, SP 800-38A	ECB	256-bit keys with 256-bit key strength	Approved Block Cipher for Counter DRBG (Cert.# A2248)
A2248	AES-ECB / FIPS 197, SP 800-38A	ECB	256-bit keys with 256-bit key strength	Prerequisite for AES-GCM (A2248)
A2248	AES-GCM/ FIPS 197, SP 800-38D	GCM[2]	256-bit keys with 256-bit key strength IV: 96 bits	Key Encryption / Decryption
A2248	Counter DRBG / SP 800-90A Rev. 1	CTR_ DRBG (AES-256)	AES 256 bits with Derivation Function Enabled	All Cryptographic Key Generation
A2248	SHA2-384 / FIPS 180-4	SHA-384	SHA-384	Message Digest for digital signature verification (Cert.# A2255)
A2249	AES-ECB / FIPS 197, SP 800-38A	ECB	256-bit keys with 256-bit key strength	Prerequisite for AES-XTS (A2249)
A2249	AES-XTS Testing Revision 2.0 / FIPS 197, SP 800-38E	XTS	256-bit keys with 256-bit key strength	Data Encryption / Decryption
A2255	ECDSA SigVer (FIPS186-4) / FIPS 186-4	Curve P-384 with SHA-384	384 bits	Digital Signature Verification
Vendor Affirmed	CKG / SP 800-133rev2 (Section 4, 6.1, 6.3)	N/A	N/A	Symmetric Cryptographic Key Generation; SP 800-133rev2 and IG D.H.
-	ENT (P) / SP800-90B	N/A	N/A	ENT (P) provides a minimum of 256 bits of entropy for DRBG seed materials in key generation.

Table 4. Approved Algorithms

Note that not all algorithms/modes that appear on the module's CAVP certificates are utilized by the module. Table 4 lists only the algorithms/modes that are utilized by the module.

[1] *Not all algorithms/modes that appear on the module's CAVP certificates are utilized by the module.*

[2] *IG C.H Scenario 2 for generating an IV is implemented in this module. In other words, Key and IV are generated internally using by approved CTR-DRBG (A2248).*

2.3.2. Non-Approved Algorithm

The module does not implement any Non-Approved Algorithms Not Allowed in the Approved Mode of Operation or Non-Approved Algorithms Allowed in the Approved Mode of Operation. The following algorithms are not intended to be used as a security function and are not implemented to meet any FIPS 140-3 requirements. Additionally, these algorithms are not provided through a non-approved service to an operator

Algorithm	Caveat	Use / Function
AES-GCM / FIPS 197, SP800-38D (non-compliant)	No Security Claimed; AES-GCM is only used for obfuscation and removal of obfuscation the CSP. (IG 2.4.A Scenario #1)	Key obfuscation and Removal of obfuscation
AES-XTS / FIPS 197, SP 800-38E (non-compliant)	No Security Claimed; AES-XTS is used to remove obfuscation from the firmware during ROM initialized.	Removal of firmware obfuscation
	No Security Claimed; AES-XTS is used for obfuscation and removal of obfuscation the CSP. (IG 2.4.A Scenario #1)	Key obfuscation and Removal of obfuscation
HMAC-SHA2-256 / FIPS 198-1 (non-compliant)	Non-approved algorithms here are only used as pre-requisite algorithms for PBKDF2 which is used for storing authentication data. (IG 2.4.A Scenario #1)	Store authentication data
PBKDF2 / SP 800-132 (non-compliant)	Non-approved algorithms here are only used for storing authentication data using PBKDF2 (IG 2.4.A Scenario #1)	Store authentication data
SHA2-256 / FIPS 180-4 (non-compliant)	Non-approved algorithm here are only used as pre-requisite algorithms for PBKDF2 which is used for storing authentication data. (IG 2.4.A Scenario #1)	Store authentication data

Table 5. Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

2.4. Approved Mode of Operation

The module only supports one mode of operation: the Approved mode, in which the Approved cryptographic functions are available. The module automatically transitions to the Approved mode of operation after completing its pre-operational self-tests. The cryptographic module indicates its approved mode through the validated version status, displayed by the Show Status Service in Table 8 via the PCIe command. In the approved mode of operation, non-approved algorithms are allowed, but with no security claims in the module.

3. Cryptographic Module Interfaces

The module does not support a Control Output Interface.

Physical port	Logical interface	Data that passes over port/interface
NVMe Connector	Data Input / Output	plaintext data; signed data
	Control Input	commands input logically via an API; signals input logically or physically via one or more physical ports
	Status Output	status information output logically via an API; signal outputs logically or physically via one or more physical ports;
	Power	N/A
JTAG	Control Input	signals input logically or physically via one or more physical ports
	Status Output	signal outputs logically or physically via one or more physical ports;

Table 6. Ports and Interfaces

4. Roles, Services, and Authentication

4.1. Role

The cryptographic module does not support role-based authentication. Roles are implicitly assumed based on the service they are invoking. The module does not support any bypass capabilities.

Role	Service	Input	Output
Cryptographic Officer (CO)	Show Status	PCIe Command	Status
	Lock/Unlock an LBA Range	LBA Range	Status
	Erase an LBA Range's Data	LBA Range	Status
	Update the firmware	FW image binary	Status
	Get Random Number	TCG Command	Status
	IO Command	LBA Range	Status
	Sanitize / DeleteNS	LBA Range	Status
	FormatNVM	LBA Range	Status
	Revert	PSID	N/A
	Perform the Self-tests	N/A	Status
	Change the Password	N/A	Status
	Set User Password	N/A	Status
	Authentication	N/A	Status
Maintenance[3]	Diagnostics	N/A	N/A

Table 7. Roles, Service Commands, Input and Output

4.2. Service

4.2.1. Approved Service

The cryptographic module only supports the following approved services and does not support any non-approved services. The abbreviations of the type of access to keys and SSPs have the following interpretation:

- E = Execute: The module performs approved security functions with the SSPs.
- G = Generate: The module generates or derives the SSP.
- W = Write: The SSP is updated, imported, or written to the volatile storage specified in Table 12.
- Z = Zeroise: The module zeroises the SSP.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs				Indicator[4]
					E	W	G	Z	
Show Status	Show approved version status and version information of the module / Error State in operational state	N/A	N/A	CO	-	-	-	-	NVM Command: Identify Controller command Result : Status Code
Lock/Unlock an LBA Range	Block or allow read (decrypt) / write (encrypt)	AES-GCM / A2248	MEK			O		O	UID: Locking_GlobalRange / Locking_RangeNNNN
			KEK		O	O		O	

[3] *Maintenance role is an operator responsible for using the JTAG.*

[4] *The result of ATA or TCG command is used as an indicator.*

	of user data.								TCG Method: Set Result: TCG status code
Erase an LBA Range's Data	Erase user data by changing the data encryption key.	Counter DRBG / A2248 AES-ECB / A2247	DRBG V DRBG Key DRBG Seed Entropy Input String		O	O	O	O	UID: K_AES_256_GlobalRange_Key / K_AES_256_RangeNNNN_Key TCG Method: GenKey Result: TCG status code
		AES-GCM / A2248 CKG ENT (P)	MEK			O	O	O	
Update the firmware	Update the firmware	ECDSA SigVer (FIPS186-4) / A2255 SHA2-384 / A2248	FW Verification Key		O				Admin Command: Firmware Commit Result : Status Code
Get Random Number	Provide a random number generated by the CM.	Counter DRBG / A2248 AES-ECB / A2247	DRBG V DRBG Key DRBG Seed Entropy Input String		O	O	O	O	UID: ThisSP TCG Method: Random Result: TCG status code
IO Command	Read/Write user data	AES-XTS Testing Revision 2.0 / A2249	MEK		O				NVM Command: Write / Read Result : Status Code
FormatNVM	Erase user data by changing the data encryption key.	Counter DRBG / A2248 AES-ECB / A2247	DRBG V DRBG Key DRBG Seed Entropy Input String		O	O	O	O	Admin Command: Format NVM Result : Status Code
		CKG ENT (P)	MEK			O	O	O	
			KEK			O	O		
Sanitize / DeleteNS	Erase user data by changing the data encryption key.	Counter DRBG / A2248 AES-ECB / A2247	DRBG V DRBG Key DRBG Seed Entropy Input String		O	O	O	O	Admin Command: Sanitize / Namespace Management Result : Status Code
		CKG ENT (P)	MEK			O	O	O	
			KEK			O	O	O	
Revert	Erase user data in all Range by changing the data	Counter DRBG / A2248 AES-ECB / A2247	DRBG V DRBG Key DRBG Seed Entropy Input String		O	O	O	O	UID: SPObj(AdminSP) TCG Method: Revert Result: TCG status code
		CKG ENT (P)	MEK			O	O	O	
			KEK			O	O	O	
Perform the Self-tests	Power cycling the module to perform self-tests	AES-XTS (No Security Claimed)	DRBG V DRBG Key DRBG Seed Entropy Input String MEK		-	-	-	O	Level 0 Discovery CMD return a failure as a failure indicator

			KEK Firmware Verification Key						
Change the Password	Change CO password	No Security Claimed – PBKDF2 (non-compliant) HMAC-SHA2-256 (non-compliant) SHA2-256 (non-compliant)	N/A		-	-	-	-	N/A
Authentication	Authenticate the module. (This is not authentication to meet the FIPS 140-3 requirements)	No Security Claimed – PBKDF2 (non-compliant) HMAC-SHA2-256 (non-compliant) SHA2-256 (non-compliant)	N/A		-	-	-	-	N/A
Diagnostics	Perform Maintenance	N/A	N/A		-	-	-	-	N/A

Table 8. Approved Services

4.3. Authentication

The module does not support any authentication mechanisms to access its services under Security Level 1.

5. Software/Firmware Security

- The integrity of the module’s executable firmware (OPP9TA6A_DC_2048.bin) is verified using ECDSA SigVer P-384 (A2255) with SHA2-384 (A2248) for firmware integrity testing of the following components:
    - Boot Loader - ECDSA SigVer P-384 (A2255) with SHA2-384 (A2248)
    - Main Firmware - ECDSA SigVer P-384 (A2255) with SHA2-384 (A2248)
- The operator can initiate the firmware integrity tests on-demand by power-cycling the module.

6. Operational Environment

- The cryptographic module operates in a limited operational environment, consisting of the module's firmware. This module does not have an operating system but is designed in a manner to allow controlled, validated firmware modifications by an operator. This operational environment does not require any specific security rules, settings, configurations, or restrictions to be set.

- The cryptographic module does not provide any general-purpose operating system to the operator.

- Firmware download is only available for CMVP validated firmware versions. Unauthorized modification of the firmware is prevented by the pre-operational firmware integrity test and conditional firmware load test.

- Since the cryptographic module is zeroised through the procedure for using maintenance role, it is restricted to prevent uncontrolled access to CSPs and uncontrolled modifications of SSPs.

7. Physical Security

The following physical security mechanisms are implemented in the cryptographic module:

- Production grade components.

The cryptographic module supports the Maintenance role. To assume the Maintenance role, operators must comply with the following rules:

- The operator must zeroise all SSPs listed in Table 11 by invoking the Revert service in the Table 8 and initiate the Power on reset before entering the Maintenance role.
- To exit the Maintenance role, the operator must procedurally perform the Revert service in the Table 8 and perform a power-on reset of the module. Finally, the operator performing the Show Status service in Table 8 confirms the original firmware version listed in the Table 3 remains unchanged.
- The operator is responsible for managing the module's JTAG port and should conduct regular inspections associated with the enabled JTAG port as frequently as possible in order to prevent potential security risks such as potential code modifications with no firmware load test, reading and writing of register information or other impactful security changes.

8. Non-Invasive Security

- The module does not implement any non-invasive attack mitigation techniques. Therefore, this section is not applicable.

9. Sensitive Security Parameters Management

- Temporary SSPs and SSPs stored in volatile memory are automatically zeroized upon power-on reset.
- The module performs zeroization by overwriting the target SSP with random values generated by the DRBG.
- The module does not import or export SSPs.
- All SSPs in volatile memory, including HW SFR, are automatically zeroised instantly either after key generation/use or upon performing power-on-reset, depending on the characteristics of volatile memory.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establish -ment	Storage	Zeroisation[5]	Use & related keys
DRBG V / CSP	128-bit	Counter DRBG / A2248 AES-ECB / A2247	SP 800-90A Rev. 1 Counter DRBG	N/A	N/A	Plaintext in RAM	Explicitly zeroised via these services: Performing via Erase an LBA Range's Data, Sanitize / DeleteNS, FormatNVM, and Revert service, and zeroisation is shown through their respective indicator. Implicitly zeroised by Power on Reset	Generates the MEK and KEK
DRBG Key / CSP	256-bit	Counter DRBG / A2248 AES-ECB / A2247	SP 800-90A Rev. 1 CTR_DRBG (AES-256)	N/A	N/A		Explicitly zeroised via these services: Performing via Erase an LBA Range's Data, Sanitize / DeleteNS, FormatNVM, and Revert service, and zeroisation is shown through their respective indicator. Implicitly zeroised by Power on Reset	Generates the MEK and KEK
DRBG Seed / CSP	384-bits	Counter DRBG / A2248	ENT (P) CKG	N/A	N/A		Explicitly zeroised via these services: Performing via	Generates the MEK and KEK

[5] *"Zeriosation" performs in non-volatile memory.*

		AES-ECB / A2247					Erase an LBA Range’s Data, Sanitize / DeleteNS, FormatNVM, and Revert service, and zeroisation is shown through their respective indicator. Implicitly zeroised by Power on Reset	
DRBG Entropy Input String / CSP	384-bits	Counter DRBG / A2248 AES-ECB / A2247	ENT (P) CKG	N/A	N/A		Explicitly zeroised via these services: Performing via Erase an LBA Range’s Data, Sanitize / DeleteNS, FormatNVM, and Revert service, and zeroisation is shown through their respective indicator. Implicitly zeroised by Power on Reset	Generates the MEK and KEK
KEK / CSP	256-bit	AES-GCM / A2248	CKG SP 800-90A Rev. 1 Counter DRBG	N/A	N/A	Plaintext in RAM Obfuscated in Flash	Explicitly zeroised via these services: Performing via Sanitize / DeleteNS, FormatNVM, and Revert service, and zeroisation is shown through their respective indicator. Implicitly zeroised by Power on Reset	Wraps MEK
MEK / CSP	256-bit	AES-XTS Testing Revision 2.0 / A2249	CKG SP 800-90A Rev. 1 Counter DRBG	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on Reset	Data encryption and decryption of user data
						Cipher text in Flash	Explicitly zeroised via these services: Performing via Erase an LBA	

							Range's Data, Sanitize / DeleteNS, FormatNVM, and Revert service, and zeroisation is shown through their respective indicator.	
Firmware Verification Key[6] / PSP	192-bit	ECDSA SigVer (FIPS186-4) / A2255 SHA2-384 / A2248	Entered during manufacturing	N/A	N/A	Plaintext HW SFR[7]	Explicitly zeroised via this service: Performing via Update the Firmware service, and zeroisation is shown through their respective indicator.	Firmware Load Test
						Plaintext in ROM	N/A	

Table 9. SSPs

The cryptographic module contains an entropy source, compliant with SP 800-90B.

Entropy sources	Minimum number of bits of entropy	Details
ENT (P)	384 bits	The entropy source provides an estimated min-entropy output of 0.5[8] bits per bit. The DRBG is seeded with 768 bits of entropy input data from the entropy source. Therefore, the DRBG is seeded with at least 384-bits of entropy before generating SSPs.

Table 10. Non-Deterministic Random Number Generation Specification

[6] **Note: This is not considered an SSP as per ISO/IEC 19790:2012 section 7.5 but is included in the list for completeness.*

[7] *HW SFR (Special Function Register) is a register within a hardware cryptographic algorithm IP, which has characteristic of volatile memory.*

[8] *Estimated amount of entropy per the source ́s output bit is 0.85444 and Samsung conservatively claims to be set at 0.5 per bit.*

10. Self-Tests

While executing the following self-tests, all data output is inhibited until the completion of the self-test. Conditional self-tests are conducted before the initial operation of approved algorithms. If a cryptographic module fails a self-test, it will enter an error state, during which all data output is inhibited.

10.1. Pre-operational test

Algorithm	Type	Description
ECDSA	Firmware integrity test	Firmware integrity test for Boot Loader is performed by using ECDSA with SHA2-384 at every power-on-reset.
ECDSA	Firmware integrity test	Firmware integrity test for the Main Firmware is performed by using ECDSA with SHA2-384 at every power-on-reset.

Table 11. Pre-operational Self-tests

10.2. Conditional test

Algorithm	Type	Description
AES-XTS	Critical Function Test	Duplicate Key Test for AES-XTS described in FIPS 140-3 IG C.I (i.e. key_1 ≠ key_2)
AES-XTS	Cryptographic algorithm self-test	KAT: Encrypt is performed (256-bits)
AES-XTS	Cryptographic algorithm self-test	KAT: Decrypt is performed (256-bits)
ECDSA	Cryptographic algorithm self-test	KAT: Curve P-384 with SHA-384 signature verification is performed
SHA2-384	Cryptographic algorithm self-test	KAT: Hash digest is performed
CTR DRBG	Cryptographic algorithm self-test	KATs: SP 800-90A Rev. 1 Health testing on Instantiate, Generate and Reseed functions
CTR DRBG	Cryptographic algorithm self-test	KAT: DRBG with AES-256 is performed
AES-GCM	Cryptographic algorithm self-test	KAT: Encrypt is performed
AES-GCM	Cryptographic algorithm self-test	KAT: Decrypt is performed
ECDSA	Firmware load test	ECDSA signature verification is performed if new FW is downloaded or at every power-on-reset
ENT (P)	Cryptographic algorithm self-test	Conditional SP800-90B Health tests: Repetition count test, Adaptive proportion test

Table 12. Conditional Self-tests

10.3 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error state in Boot	The module has failed any self-tests during the boot	During the boot	Power cycle	The module is not initiated, so no services are available.
Error State in operational state	The module has failed any self-tests in the	Transition to approved mode of operation Operational state	Power cycle	ERRORMOD message in Show status service

	operational state			

Table 13: Error States

11. Life-Cycle Assurance

The cryptographic module operates in the Approved mode of operation by default upon shipment from the vendor's manufacturing site and does not support a non-approved mode of operation. Section 11.1 provides guidance on the rules for secure installation and operation. Operators must follow this guidance to ensure the cryptographic module operates in compliance with FIPS 140-3 security level 1 requirements.

11.1. Secure Installation

- Identify the firmware version in the device
  - Confirm that the firmware version is equivalent to the version(s) listed in this document via NVM express Identify Controller command.

11.2. Operational Description of Module

- The cryptographic module shall maintain logical separation of data input, data output, control input, status output, and power.
- The cryptographic module shall not output CSPs in any form.
- The cryptographic module shall use the Approved DRBG for generating all cryptographic keys.
- The cryptographic module shall enforce a limited operational environment by the secure firmware load test using ECDSA with SHA-384.
- The cryptographic module shall provide a production-grade cryptographic boundary.
- The Cryptographic module enters the error state upon failure of Self-tests. most commands except for supported command from the Host (General Purpose Computer (GPC) outside the cryptographic boundary) are rejected in the error state and the IO command returns Namespace Not Ready (SC=0x82, SCT=0x0), the other commands return Internal Error (SC=0x6, SCT=0x0) defined in NVMe specification via the status output. Cryptographic services and data output are explicitly inhibited when in the error state. When the module fails FW Integrity test performed by Mask ROM, the module will fail to boot; module will not service any requests or provide any status output (module hangs).
- The cryptographic module satisfies the requirements of FIPS 140-3 IG C.I (i.e. key_1 ≠ key_2)
- The module generates at a minimum 256 bits of entropy for use in key generation.
- Bypass capability is not applicable to the cryptographic module.
- The module generates symmetric keys which are unmodified outputs from the DRBG.
- As specified in NIST SP 800-132, keys derived from passwords/passphrases may only be used in storage applications.
- AES-XTS is only approved for storage applications.
- If you require the "Samsung SED Product Manual", kindly reach out to the vendor contact information that is posted in certification.

12. Mitigation of Other Attacks

The cryptographic module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-3.